

AO 106 (Rev. 04/10) Application for a Search Warrant Agent: AUSA: Mark Chasteen Telephone: (313) 226-9555  
Matthew Lariviere Telephone: (313) 912-6881

## UNITED STATES DISTRICT COURT

for the  
Eastern District of Michigan

In the Matter of the Search of )  
(Briefly describe the property to be searched )  
or identify the person by name and address) )  
2 Black I-phones; Mac Book; and Samsung Galaxy cell )  
phone )  
See Attachments for description. )

Case: 2:19-mc-50420  
Assigned To : Michelson, Laurie J.  
Assign. Date : 3/21/2019  
Case No. Description: RE: SEALED MATTER  
(EOB)  
1

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See ATTACHMENT A.

located in the Eastern District of Michigan, there is now concealed (identify the person or describe the property to be seized):

See ATTACHMENT B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

18 U.S.C § 371, 514

Conspiracy; Make, utter, posses counterfeit security/checks.


18 U.S.C § 1343, 1029

Wire Fraud, Access device fraud

The application is based on these facts:

See attached AFFIDAVIT.

- ☒ Continued on the attached sheet.  
☐ Delayed notice        days (give exact ending date if more than 30 days:       ) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Matthew Lariviere - Special Agent

Printed name and title

Sworn to before me and signed in my presence  
and/or by reliable electronic means.

Date: March 21, 2019

City and state: Detroit, Michigan



Judge's signature

David R. Grand

U. S. Magistrate Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Matthew D Lariviere, being first duly sworn, hereby depose and state the following:

- (1) I make this affidavit in support of an application for a warrant to search the following electronic devices that are in the custody of the United States Secret Service in Detroit, Michigan:
  - (a) a black Apple iPhone IMI #356769087236816 seized by the West Bloomfield Township Police Department on February 9, 2018;
  - (b) an Apple Macbook laptop computer (serial number C02VG2HFHH27) seized by the West Bloomfield Township Police Department on February 9, 2018;
  - (c) an Apple iPhone, IMI#354856093929633, seized by the Huron Township (Michigan) Police Department on August 25, 2018.
  - (d) a Samsung Galaxy mobile phone, IMI #359754071351554 seized by the Huron Township (Michigan) Police Department on August 25, 2018.

- (2) I am a Special Agent with the United States Secret Service assigned to the Detroit Field Office. I have been employed in this capacity since January 2015. I am currently assigned to the Electronic Crimes Task Force. I have participated in numerous investigations involving counterfeiting, bank fraud, mail fraud, wire fraud, computer fraud and access device fraud.
- (3) The information contained in this affidavit is based on my training, experience, and participation in financial crime and counterfeit investigations, as well as from personal observations during the course of this investigation. Information was also provided by law enforcement officers and others who have personal knowledge of the events and circumstances described herein.
- (4) Because this affidavit is being submitted for the limited purpose of establishing probable cause, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that the

evidence described in Attachment B is currently present in the location described in Attachment A. The aforementioned property is currently in the custody of the U.S. Secret Service (USSS), as further specified in Attachment A.

- (5) The items referred to in Attachment B and sought to be seized constitute evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 371, (conspiracy), 514 (fictitious obligations, security, make, utter, possess counterfeit security/check: make, utter, possess a forged security/check), 1343 (wire fraud), 1344 (bank fraud), and 1029 (access device fraud) (hereinafter “the Specified Federal Offenses”).

#### SUMMARY OF INVESTIGATIVE FINDINGS

- (6) My investigation has shown Ezel McElroy is responsible for organizing a counterfeit fraud ring and scheme involving Fifth Third Bank, PNC Bank, Comerica Bank, and other banks that has been ongoing since January 2018. McElroy has been manufacturing and passing counterfeit checks in Michigan and Georgia and has conspired with others and been aided and abetted by others in his scheme. Although

variations exist in particular transactions, the basic scheme is this: McElroy and others with whom he has conspired, or aided and abetted, solicit people with bank accounts to provide their account information, including account numbers, online login information, and debit cards, in exchange for money. These solicitations have been done through online postings on accounts belonging to McElroy and co-conspirators (such as Instagram), or text messages, followed by telephone conversations or text messages with the bank account holders to arrange for transfer of their account information and debit card. McElroy, his co-conspirators, or accomplices, then cause counterfeit checks to be deposited into the bank account. McElroy or others withdraw funds from the account a short time later, when the deposited funds are available for withdrawal, but before the banks have discovered the deposited checks are counterfeit. McElroy has been investigated and arrested by Huron Township and West Bloomfield Police Departments for check fraud, identity theft, and possession of fraudulent financial access devices. All told,

financial institutions have attributed \$1.5 million in potential loss and \$600,000.00 in actual loss to McElroy through the check number, check maker, cellular metadata and security video footage.

### **PROBABLE CAUSE**

#### **Fraudulent Activity at Fifth Third Bank**

- (7) I have learned the following from Susan Clayton, an investigator employed by Fifth Third Bank. Between March 8 and March 27, 2018, eight counterfeit checks totaling \$38,319.12 were deposited into various customers' accounts, each typically in the amount of \$4,765.13 and nominally drawn from Massachusetts Mutual Life Insurance account 67937 at Bank of America. Based on surveillance, the person making the deposits was not the account holder. The deposited funds were later withdrawn via point of sale debit card transactions.
- (8) Later, additional similar fraudulent transactions occurred at Fifth Third, using different counterfeit checks, but involving 71 customer accounts and deposits of 117 fraudulent checks

in amounts between \$4,000 and \$5,000, totaling \$556,118.09 deposited through July 9, 2018. Mark D. Hobson was one customer into whose accounts a counterfeit check was deposited.

- (9) Investigator Clayton reported that by October 16, 2018, a total of \$940,125.92 in fraudulent checks had been deposited. Funds commonly were withdrawn at two check cashing stores in Detroit, including Boulevard Check Cashing and Woodward Check Cashing. Clayton identified Ezel McElroy as an individual involved in the counterfeit check fraud scheme. Clayton obtained a driver license from Shirley Hamby, an investigator at Comerica Bank, and was able to use the bank footage from Fifth Third and compared it to a driver license that was recovered from McElroy after he attempted to pass a counterfeit check at Comerica Bank.

Fraudulent Activity at Comerica Bank

- (10) I have also received information from Shirley Hamby, On March 19, 23, 26, and 29, and April 11, 2018, deposits or attempted deposits were made of counterfeit checks in

Comerica customer accounts, each in the amount of \$4,765.13 nominally from Mass Mutual and drawn on Bank of America account 67937—the same account number used for some of the counterfeit checks deposited with Fifth Third bank. Each transaction was made using a different Comerica Bank customer's account and at a different location. Funds were withdrawn from the accounts within three days of the deposits on March 19, 23, and 26 and April 11, 2018.

- (11) Between May 7 and May 21, 2018, deposits of seven counterfeit checks were made into Comerica accounts, each in the amount of \$4,972.33 and nominally drawn on Bank of America from Mass Life account 67937. Six of the seven deposits were made into an account of a different customer, and the deposits were made at five different locations. Funds usually were withdrawn from the accounts within 1–2 days. On May 11, 2018, an attempted deposit of a counterfeit check in the amount of \$4,972.33, nominally drawn on Bank of America from Mass Life account 67937, was made at a Comerica Bank location. The person who attempted to make



the deposit fled the location, leaving the check behind.

- (12) On June 20 and June 21, 2018, three separate deposits or attempted deposits of counterfeit checks drawn on Sterling Bank and Trust, account 67937, from CMAI Industries, each for \$4,831.70, were deposited into a Comerica account in the name of B.B. Each deposit was made at a different Comerica Bank branch location. On June 21, 2018, ATM withdrawals totaling \$4,500 were made at Boulevard Check Cashing in Detroit. Another ATM withdrawal for \$320 was made at an ATM in Detroit. On June 22, 2018, B.B. went to a Comerica Bank location in Oak Park and attempted to withdraw \$2,000.00.
- (13) B.B. told Shirley Hamby that she replied to an Instragram message: "if you have a bank account and would like to earn a few extra bucks . . . hit me up" from Instragram profiles @BIIGTAE and @the Real Crispy E. B.B. stated she did not know who @BIIGTAE was, but @the Real Crispy E was Ezel McElroy, with whom she had attended Oak Park High School. The person associated with the @BIIGTAE profile came to

B.B.'s home, and she gave him her ATM card and account number.

- (14) On June 26 and July 6, 2018, additional deposits of counterfeit checks drawn on Sterling Bank & Trust account 67937 in the amount of \$4,831.70 were deposited into the Comerica bank accounts of two other customers. Withdrawals of funds totaling \$4,800 and \$2,500 were made from the two accounts within days of the deposits.

Fraudulent Activity at PNC Bank

- (15) On October 17, 2018, PNC Bank Investigator Carol Crane contacted SA Tyler Bennett and I to provide information into an organized check fraud ring involving counterfeit life insurance checks. Crane stated that from April 9, 2018 to - September 27, 2018 a total of 88 transactions occurred involving the depositing of counterfeit checks into 59 checking accounts for the amount of \$799,231.58. With some exceptions, the checks ranged from \$4,200.00 to \$9,938.37. A total of \$213,187.87 was withdrawn from the 59 accounts. Multiple counterfeit checks that were deposited contained the

same company name, check number and account numbers.

Many of the checks that were deposited contained the same information as the checks deposited at Fifth Third and Comerica. Video surveillance showed that checks were deposited into individual accounts by the account holders themselves and members of the organized check fraud ring. Following the deposits, funds were depleted via point of sale debit card transactions, wire transfers and cash advances throughout the Detroit area. Ezel McElroy was identified as one of the individuals associated with depositing of counterfeit checks and withdrawing funds from ATMs.

West Bloomfield Township Police Department  
Investigation and Arrest of Ezel McElroy

(16) I have reviewed police reports, as well as search warrant applications, from the West Bloomfield Township (Michigan) Police Department (WBPD) and the Huron Township (Michigan) Police Departments, and met with WBPD Detective Erik Hamilton.

(17) In the course of an investigation into a home invasion and armed robbery that occurred on January 30, 2018 at XXX2

Silverbrooke West in West Bloomfield Township, WBPD determined that Ezel McElroy and his brother Blake Benford lived at that location. K.P. was a suspect in the home invasion and armed robbery. K.P. told WBPD detectives that Ezel McElroy used K.P.'s paycheck from Covenant Construction to create counterfeit checks.

(18) Detective Hamilton interviewed K.P. on February 5, 2018.

K.P. stated that he knows Ezel McElroy. About one month prior to the interview, K.P. received a direct message from McElroy through Instagram. McElroy inquired about K.P.'s JP Morgan Chase bank account and asked if K.P. wanted to make money. McElroy asked for K.P.'s bank card, personal identification number, and online banking login so McElroy could deposit a "QuickPay" of \$2,000–\$3,000 into K.P.'s account. QuickPay is a mobile banking feature that allows users to deposit checks into their accounts remotely. McElroy said he would need K.P.'s bank card for a day or two, and K.P. would receive \$500 for letting McElroy use the account. K.P. met McElroy at a gas station in Southfield, Michigan on

January 1, 2018 and gave McElroy his bank card and online banking information. A few days later, McElroy told K.P. the QuickPay did not go through.

- (19) Around January 19-20, 2018, McElroy asked KP if he knew anyone with a bank account because KP's account was not "poppin."
- (20) K.P. stated a "Chris Financial" check in his account was from his employer Covenant Construction. K.P. thought McElroy found it while signed into his account. McElroy told K.P. he "remade" the check using account and routing numbers on K.P.'s check. McElroy told K.P. he was writing checks of \$4,700 and making them payable to random people who were then "dropping" the checks into their accounts. Detective Hamilton reviewed a report from the Clinton Township Police Department in which the owner of Covenant Construction reported that he had been informed by Christian Financial that a number of fraudulent checks had been cashed.
- (21) K.P. heard that McElroy downloaded a program that contains different formats for checks so he just had to input names and

account numbers. K.P. recalled seeing a laptop computer connected to a printer inside McElroy's residence at XXX2 Silverbrooke West that McElroy used to print checks.

McElroy asked K.P. if he could get check paper and magnetic ink.

(22) K.P. identified Instagram account "therealcrispye\_" as belonging to Ezel McElroy.

(23) On February 6, 2018, Detective Hamilton reviewed the Instagram account therealcrispye\_ and saw photographs of a black male consistent with Ezel McElroy. On February 6, therealcrispye\_ posted "Who got a 700+ credit score and wanna make 5,000" and "who got a 600+ credit score and wanna make 3-5k."

(24) On February 9, 2018, officers from the WBPD went to XXX2 Silverbrooke West to execute a search warrant obtained from the 48th District Court. As they approached, officers saw an occupied Nissan Pathfinder running at the curb in front. Mark Hobson was walking from the direction of the apartment. When asked where he was coming from, Hobson

indicated he had come from a nearby apartment and stated he had not come from XXX2. Based on tracks in newly fallen snow, it appeared Hobson had come from the entry door of XXX2, not the apartment he indicated. Ezel McElroy was seated in the driver's seat of the Pathfinder. Another person, Mack C., was in the front passenger seat. A query showed the Pathfinder was listed as stolen by the Wayne County Airport Authority on February 2, 2018.

- (25) Ezel McElroy and Mack C. were arrested and transported to the WBPD station. McElroy was searched and found to be in possession of a Huntington Bank credit card bearing the name of N.B. and a card number ending in -1482.
- (26) Detective Runsat of the WBPD searched the Pathfinder and found: a Huntington Bank deposit receipt dated February 8, 2019, in the amount of \$4784.43 into account ending in -0315; a transaction record receipt dated 2/9/18 at 02:48 hours with card ending in -1482; a fraudulent Safeco Insurance Company check #82349 in the amount of \$4,784.43 and dated January 6, 2018, made payable to Z.T.; and a birth certificate and

traffic citation for Mark Hobson.

(27) Detective Hamilton spoke with Huntington Bank investigator Jason Meggie, who stated that N.B. had an account at Huntington Bank ending in 0315 and a deposit of \$4,784.43 was made into N.B.'s account on February 8, 2018, which was not consistent with N.B.'s everyday banking activity.

Detective Hamilton spoke with N.B., who reported that she lost her Huntington Bank debit card approximately two days earlier. Later, in June 2018, N.B. told Detective Hamilton that she received a text message from an unknown number asking about her debit card. She spoke with the person who sent the text and agreed to give her debit card so they could deposit a check. Shortly after that, two tall black males arrived at her home and she gave them her debit card and PIN.

(28) Detective Hamilton reviewed an Apple iPhone belonging to Mack C. on February 13, 2018, and found text and email messages, and photographs, containing names, addresses, account, account login information, and transactions at



several different banks. Detective Hamilton also found:

- (a) a text conversation in which a phone number ending in - 5446 sent several pictures containing the personal identifying information of different people;
- (b) a picture of N.B.'s address and Huntington Bank login and password, received on February 6, 2018. (Messages around the picture discussed when to pick up N.B.'s card and depositing a check.);
- (c) a photograph dated January 14, 2018 showing an unknown online bank account with balances of \$5,842.56 and \$20,000.00. (It appeared the photograph was posted to therealcrispye's Instragram page where written across the photograph is, "My lil nigga Mack go so crazy.");
- (d) a photograph dated 1/10/18 from mcelroyezel@icloud.com where McElroy sent Mack C. a text message via icloud with a username and password for D.L., as well as D.L.'s address and county of residence;
- (e) in an Instagram album, several photographs soliciting someone with a bank account who wants to make money.

(29) Officers of the WBPD searched XXX2 Silverbrooke West on February 9, 2018, pursuant to the search warrant and found documents associated with Ezel McElroy in the southeast bedroom. In that bedroom, officers also found:

- (a) several mobile phones, including a black Apple iPhone with IMI #356769087236816, currently in the custody of the United States Secret Service in Detroit, Michigan);
- (b) a Huntington MasterCard in the name of D.H.; and
- (c) Christian Financial cards in the name of A.Z. and M.P.

(30) In the dining room of XXX2 Silverbrooke West, officers found a HP laptop computer with a camouflage pattern, a HP laser jet printer, two printed checks, and a box of blank payroll checks with no checking account information printed on the face. In the living room, officers found a rose-colored Apple Macbook computer, serial number C02VG2HFHH27 (currently in the custody of the United States Secret Service in Detroit, Michigan).

(31) WBPD Detective St. Germaine contacted D.H., whose Christian Financial card was found in Ezel McElroy's

bedroom. D.H. stated he did not give any other person permission to have his bank card. D.H. stated his account was cancelled after a check was cashed fraudulently on his account.

(32) On February 10, 2018, Detective Hamilton interviewed D.B., who was sleeping on the living room couch when officers entered XXX2 Silverbrooke West on February 9. D.B. stated the following:

- (a) Ezel McElroy, Blake Benford, and Moses McElroy all used the camouflage laptop computer officers found on the dining room table.
- (b) D.B. had seen checks on the printer but could not say who printed them because multiple people use the printer.
- (c) After checks are printed, they are placed into an envelope to make them look like payroll checks.
- (d) After a check is cashed, Ezel McElroy and Benford take half of the money and the person who cashed it receives the other half. The check will then be “dropped” a second time, and split again, so that Ezel McElroy and Benford

receive the full amount of \$4,783.43.

(e) The most commonly used banks are Bank of America, Huntington Bank, and Michigan First Credit Union, but they will use all banks and have been pretty successful.

(33) On or about February 9, 2018, WBPD Detective St. Germaine contacted A.Z., whose Christian Financial card was found in Ezel McElroy's bedroom. At that time, A.Z. stated he did not give any other person permission to have his bank card and that an unknown person applied for another card in his name without his knowledge and tried to change his email.

Detective Hamilton spoke with A.Z. again on February 16, 2018. A.Z. said a few weeks earlier an acquaintance, B.W., advertised on his Snapchat account that he was looking for anyone with an active bank account who wanted to make money. A.Z. met with B.W., who pressured him into giving B.W. his Christian Financial debit card and access to his bank account to cash a check. A few days later, Christian Financial informed A.Z. that a fraudulent check had been deposited into his account.

(34) On or about February 20, 2018, Detective Hamilton did a preview of the camouflage HP laptop found in the dining room of XXX2 Silverbrooke West, and found that the Checksoft program had been installed. A Google search showed that Checksoft is used to design and print personal, business, and payroll checks.

(35) On April 9, 2018, Detective Hamilton reviewed the rose-colored Apple Macbook found in the living room of XXX2 Silverbrooke West. The Macbook contained a user profile for Ezel McElroy that was password locked. Hamilton used a password previously provided by McElroy and unlocked the computer. The email and messaging applications automatically opened. Among other evidence of identity theft and bank fraud, Detective Hamilton saw:

(a) messages to or from two different telephone numbers in which over 300 customer profiles for T-Mobile accounts containing personally identifiable information, including name, address, DOB, phone number, username, password, and some complete social security numbers were

exchanged;

(b) a February 5, 2018 screen shot of a sample State of Wisconsin check;

(c) a February 5, 2018 screen shot of a Bank of America online account showing a deposit of a State of Wisconsin Income Tax Refund check payable to T.W. in the amount of \$1,301.64;

(d) a photograph dated February 6, 2018, showing a check in the amount of \$980.56 payable to T.W., drawn on the TD Bank account of Future Project DD Department;

(e) a Gmail account for crispygang24@gmail.com in the internet history.

(36) On April 10, 2018, Detective Hamilton spoke with a manager at TD Bank, who advised that Future Project DD Department had experienced fraudulent checks being cashed, leading to its account being frozen. Detective Hamilton subsequently received a phone call from A.G., who identified himself as the owner of Future Project, and who confirmed his business had experienced fraudulent checks in Detroit, Michigan and

Orlando, Florida, and stated neither he nor his company had employed T.W. Detective Hamilton located a phone number for T.W. and spoke with a female who identified herself as T.W. T.W. said 2–3 months earlier she experienced fraud on her Bank of America account where three fraudulent checks were deposited into her account. T.W. at first denied involvement, then said she was propositioned by a friend, B.M., about giving her online banking information and debit card and was promised \$1000 for the use of her account. B.M. was going to give her information to a friend who would deposit checks into her account.

(37) On April 18, 2018, Detective Hamilton examined the camouflage HP laptop found in the dining room at XXX2 Silverbrooke West on February 9, 2018. The laptop had nine user accounts, including one for “Crisp” with a full username of “crispy e cg 24”. On January 15, 2018, the user Crisp downloaded CheckSoft V14.0.1 business edition, as well as the CheckDesigner.pdf user guide. An HP printer was installed on the computer. Google searches using the Crisp

user profile included: “what sites let you pay with checking,” “check fraud protection,” “genuine original watermark,” “original genuine check,” “Safeco Insurance,” and “check fraud protection symbol.”

(38) On August 21, 2018 48th District Court (Michigan) Judge Barron found probable cause on a criminal complaint charging McElroy with one count of obtaining, possessing, or transferring personal identifying information with intent to commit identity theft and two counts of financial transaction device fraud and signed a warrant for his arrest.

Arrest of Ezel McElroy and Mark Hobson  
by the Huron Township Police Department

(39) On August 25, 2018 Officer Sheehan of the Huron Township (Michigan) Police Department stopped a Dodge Charger that was traveling southbound on I-275 at 105 miles per hour. Ezel McElroy was driving the Charger, and Mark Hobson was in the front passenger seat. McElroy and Hobson were arrested on outstanding warrants. At the time of his arrest, McElroy had in his possession an Apple iPhone,



IMI#354856093929633. Hobson had a Samsung Galaxy mobile phone, IMI #359754071351554. Both phones currently are in the custody of the United States Secret Service in Detroit.

(40) Officers searched the Charger and found a bag on the.

passenger side floor, at Hobson's feet. The bag contained:

- (a) a card scanner capable of being Bluetooth linked to any Bluetooth capable smart phone for the purpose of reading and writing to cards from the phone;
- (b) a bank statement from Fifth Third showing four different checks payable to Hobson, all returned to Hobson due to fraudulent activity. The statement showed the checks being cashed four consecutive days for approximately \$4,900 each;
- (c) a statement showing Hobson's account overdrawn by approximately \$14,000;
- (d) 13 credit cards. A magnetic strip scan showed that 10 of the cards had different numbers in the magnetic strip than showed on the face of the card, two did not scan, and

one registered to Hobson and the strip matched the face.

(41) In the trunk of the Charger, officers found:

- (a) an Amazon box containing several hundred blank checks, in three different types with security features which can be found on counterfeit checks passed at Fifth Third, PNC, and Comerica banks;
- (b) a Chase bank card with no name and a Fifth Third Bank card in the name of a person other than McElroy or Hobson.

Southfield Police Department Arrest

(42) I have also reviewed a report from the Southfield Police Department detailing an arrest of Ezel McElroy. On July 9, 2018, McElroy was arrested by the Southfield Police Department after officers observed him driving recklessly in a Dodge Charger SRT Hellcat. The report states that McElroy was the sole occupant of the vehicle and an inventory search of the vehicle revealed seven credit cards belonging to seven different individuals in the center console. A Bank of America check nominally drawn on the account of DLanzo Plumbing

and Sewer and payable to Ariana McDuffle for \$14,525.09 was found in the glove compartment. A search incident to arrest revealed \$5,961.76 in cash in McElroy's front left pocket. McElroy stated that he sells cars for his uncle and gets paid in cash.

- (43) The owner of the DLanzo Plumbing and Sewer company, D.L., was contacted regarding the check found in McElroy's possession. D.L.said that he did not know Ariana McDuffle, the name payable on the check, and he contacted his bank to see if any checks were made payable to Ezel McElroy. D.L.discovered that none of the checks were made payable to McElroy, but over \$25,000 in fraudulent checks had been cashed. On March 12, 2019, I spoke with D.L. and he stated the check is in fact counterfeit and it was not written by his company.

- (44) At the time of his arrest but the Southfield Police Department, McElroy had in his possession several bank debit cards in the name of other people. Three of the cards

were for accounts that were closed after a counterfeit check was deposited.

Other Facts Supporting Probable Cause

- (45) Mark Hobson opened a Fifth Third checking account on May 29, 2018. Four counterfeit checks were deposited in Hobson's account in the approximate amount of \$4,800.00 each, starting on June 4, 2018 through June 7, 2018. Based on the bank security footage provided by Fifth Third Bank Investigator Clayton and a list of deposits into Hobson's account, I was able to determine he did not personally make any of the deposits. ATM camera footage shows McElroy withdrawing funds from Hobson's account.
- (46) On August 27, 2018, C.F., who was then 15 years old, went to the WBPD station and reported he lost his debit card a few weeks earlier and that someone impersonated him and withdrew money from his Chase account. C.F. later admitted to Detective Kase that he did not lose his card. Instead, he saw an Instagram post by "@biigtæ" advertising that he could make anyone \$3,500 within a day. C.F. responded via direct

message. The subject said C.F. would need to provide his personal information, bank account information, and a debit card where the money could be deposited into his account.

C.F. met with the person depicted on the Instagram account on July 16, 2018 and gave him his debit card. On July 17, 2018, \$3,500 was deposited into C.F.'s account, and immediately withdrawn and transferred by an unknown person.

(47) Detective Kase obtained photos of the fraudulent ATM withdrawal from a Chase investigator. C.F. did not recognize the person in the ATM photos, noting that his physical characteristics were not consistent with "@biigtae." C.F. suggested he might be able to locate the subject from @biigtae's Instagram followers. Detective Kase noted @biigtae had over 44,000 followers, but C.F. provided the profile for "@therealcrispye" within seconds. Detective Kase recognized the page as belonging to Ezel McElroy. Based on a vehicle license plate in a photo on the Instagram account and Gray's Secretary of the State photo, it appears @biigtae belongs to

Deonte Gray. Ezel McElroy posts music videos on YouTube under the moniker The Real Crispy E.

(48) A post on the Instagram account biigtae by “the realcrispye\_” says “My boy” and shows a photo of a black male wearing a gold chain with a “CRISPY E” pendant. I recognized the black male wearing the “Crispy E” chain as McElroy. HPD took possession of the “Crispy E” chain at the time of his arrest and subsequently turned it over to WBPD where it remains in their custody.

(49) McElroy also goes by the name Crispy E, and has an Instagram account in the name of @realcrispyE\_. Messages and posts recruiting individuals to make quick cash, and images of McElroy driving Hellcat Dodge Chargers and in possession of large sums of US currency are posted on his Instagram account.

(50) Interviews conducted by Fifth Third Bank Investigator Clayton during this investigation identified PERSON A who stated at @realcrispyE\_ was the account used to coordinate the check fraud scheme between himself and McElroy.

PERSON A stated that he viewed a money making opportunity on @realcrispyE\_'s Instagram account. PERSON A, stated that he saw McElroy at a gas station and approached him about making some money. PERSON A stated that all contact was done through the @realcrispyE\_ account. PERSON A stated that all banking information username, password, debit pin were turned over via @realcrispyE\_. PERSON A stated the card was given to McElroy in person.

Use of Mobile Devices to Further the Fraudulent Scheme

(51) Based on my knowledge and experience, perpetrators of check fraud use mobile phones to facilitate check fraud. "Smart phones" now have all the capabilities of computers, including the ability to connect to the internet and store large amounts of information. Mobile phones are used to store account information and to access accounts through the internet and via banking apps. Mobile phones also are also used access, post on, and communicate through social media sites, such as Instagram, to discuss activities and successes and to recruit

new participants. as well as to communicate while individuals are participating in fraudulent activities. Perpetrators of fraudulent schemes often communicate with co-conspirators to share account information and to provide updates on the account number(s) they are using. Mobile devices also may contain data about social media, text messages, email messages, and telephone communications between participants in a scheme and used to recruit participants in the counterfeit check fraud ring, as well as location information showing the physical proximity to locations where acts in furtherance of the scheme occurred.

- (52) As noted above, there is reason to believe Ezel McElroy and his co-conspirators and accomplices, use mobile telephones to communicate with each other and with bank account holders, to facilitate their fraudulent scheme. In addition, Fifth Third Bank Investigator Clayton provided information that any time an account is accessed via the Fifth Third website or mobile app, an identification number is generated and assigned to the electronic device. These identification



numbers are unique to the mobile device and are stored in the metadata of the device. Clayton also provided the mobile device identification name of “Ezel,” which accessed multiple accounts and was used to make several transactions involving the deposit of counterfeit checks at Fifth Third. Accordingly, evidence that a device was used in connection with a fraudulent transaction might be stored within the device.

(53) The following are examples of the kind of fraudulent transactions about which mobile devices associated with Ezel McElroy, his conspirators, or his accomplices, might contain evidence:

(a) As seen in the following images, on December 18, 2018, at approximately 5:40 p.m., McElroy was observed via security footage depositing counterfeit JP Morgan Chase United Parcel Service check #20394930, in the amount of \$6,340.13, into Deneah Parraz’s Fifth Third bank account. The deposit was made at 2090 Dunwoody Club Drive, Atlanta, Georgia. The image shows McElroy utilizing a mobile device while depositing the counterfeit check. At

approximately 5:38 p.m. a mobile device ID 58954103402989574 was used to access the account via IP address 99.203.69.113. At approximately 5:42 p.m. a mobile device ID 58954103402989574 was used to access the account via IP address 108.70.140.167.

**Digital Video Snapshot**

Site: FTGA/46324 Orchard Park BM (GA)

Camera Group: 46324 Orchard Park BM

Camera Name: ATM Overview

12/18/2018 5:40:02 PM (Eastern Standard Time)



Device Station ID: 1622

Case Note 1: DENEAH PARRAZ DEP OVERVIEW

**Digital Video Snapshot**

Site: FTGA/46324 Orchard Park BM (GA)

Camera Group: 46324 Orchard Park BM  
Camera Name: ATM 4509  
12/18/2018 5:42:25 PM (Eastern Standard Time)



Device Station ID: 1622  
Case Note 1: DENEAH PARRAZ DEP \$6,340.13

(b) As seen in the following image, on December 31, 2018 at approximately 6:28 p.m., McElroy was observed via bank security footage depositing a counterfeit JP Morgan Chase United Parcel Service check #28936352, in the amount of \$5,940.13 into Mikah Sherrill's Fifth Third bank account at an ATM in Peachtree Corners, Georgia. The counterfeit check contained several of the same security features as the unprinted checks recovered by the Huron Township Police Department. McElroy can be observed utilizing a

mobile device while depositing the counterfeit check. At approximately 6:50 p.m., a mobile device ID 5424325113262156 was used to access the account via IP address 99.203.68.97.

**Digital Video Snapshot**

Site: FTGA/46307 Peachtree Corners (GA)

Camera Group: 46307 Peachtree Corners

Camera Name: ATM 4059

12/31/2018 6:28:43 PM (Eastern Standard Time)



Device Station ID: 1764

Case Note 1: MIKAH SHERRILL DEP \$5,940.13

Case Note 2: Motion: ATM 4059

Event Recorded At: December 31, 2018 6:27:44 PM

(c) As seen in the following image, on January 1, 2019, at approximately 5:21 a.m., McElroy was observed via bank

security footage accessing Sherrill's Fifth Third bank account using a debit card ending in -2156 at an ATM located at 3670 Holcomb Bridge Road, Peachtree Corners, Georgia. The image below shows McElroy holding a mobile device as he accessed the ATM and withdrew \$800.00 from Sherrill's account. At approximately 4:54 a.m. seconds mobile device ID 5424325113262156 was used to access the account from IP address 69.221.253.185, and at approximately 5:20 a.m. a mobile device was used to access the account from IP address 208.54.40.209.

**Digital Video Snapshot**

Site: FTGA/46307 Peachtree Corners (GA)

Camera Group: 46307 Peachtree Corners

Camera Name: ATM 4059

1/1/2019 5:21:07 AM (Eastern Standard Time)



Device Station ID: 1764  
Case Note 1: MIKAH SHERRILL \$800 WD  
Case Note 2: Motion: ATM 4059  
Event Recorded At: January 1, 2019 5:20:15 AM

(d) As seen on the following image, on January 4, 2019 at approximately 6:44 p.m., McElroy was observed via security footage depositing counterfeit JP Morgan Chase United Parcel Service check #20394930, in the amount of \$5,769.43, into Danisha Willis's Fifth Third bank account. The deposit was made at 10945 State Bridge Road, Alpharetta, Georgia. McElroy can be observed utilizing a mobile device while depositing the counterfeit check. At approximately 6:53, a mobile device ID 5424325113132995

was used to access the account via IP address  
69.136.135.109.

**Digital Video Snapshot**

Site: FTGA/46317 Saddlebrook BM (GA)

Camera Group: 46317 Saddlebrook BM

Camera Name: ATM 4722

1/4/2019 6:44:25 PM (Eastern Standard Time)



Device Station ID: 1610

Case Note 1: DANISHA WILLIS DEP \$5,769.43

(e) As seen in the following imagea, on January 4, 2019 at approximately 6:05 p.m. McElroy was observed via security footage depositing two counterfeit JP Morgan Chase United Parcel Service checks: (1) check #29077894, in the amount of \$5,843.43, into Miles Lunford's Fifth

Third bank account, and (2) check #29904739, in the amount of \$5,446.43 into Darod Kelly's Fifth Third bank account. The deposits were made at 3000 Old Alabama Road, Alpharetta, Georgia. McElroy can be observed utilizing a mobile device while depositing the counterfeit checks. At approximately 6:02 p.m. a mobile device ID 58954105004807575 was used to access Lunsford's account via IP address 99.203.69.2. At approximately 6:04 p.m. a mobile device ID 5424325113253791 was used to access Kelly's account via IP address 99.203.69.2 and at approximately 6:31 p.m. a mobile device ID 5424325113253791 was used to access Kelly's account via IP address 52.203.78.102.

**Digital Video Snapshot**

Site: FTGA/46322 Haynes Bridge BM (GA)

Camera Group: 46322 Haynes Bridge BM

Camera Name: Lobby IP

1/4/2019 6:05:31 PM (Eastern Standard Time)





Device Station ID: 1611

Case Note 1: MILES LUNSFORD/DAROD KELLEY DEP  
OVERVIEW

Case Note 2: Motion: Lobby IP

Event Recorded At: January 4, 2019 6:02:35 PM

**Digital Video Snapshot**

Site: FTGA/46322 Haynes Bridge BM (GA)

Camera Group: 46322 Haynes Bridge BM

Camera Name: Lobby IP

1/4/2019 6:05:31 PM (Eastern Standard Time)



Device Station ID: 1611

Case Note 1: MILES LUNSFORD/DAROD KELLEY DEP

## OVERVIEW

Case Note 2: Motion: Lobby IP

Event Recorded At: January 4, 2019 6:02:35 PM

- (f) As seen in the following image, on January 4, 2019, at approximately 6:23 p.m., McElroy was observed via security footage depositing two counterfeit JP Morgan Chase United Parcel Service checks: (1) check #34737743, in the amount of \$5,567.73 into Donovan Green's Fifth Third bank account, and check #29038478, in the amount of \$5,843.13 into Pasionique Jackson's Fifth Third bank account. The deposits were made at 2755 Old Milton Parkway, Alpharetta, Georgia. McElroy can be observed utilizing a mobile device while depositing the counterfeit check. At approximately 6:29 p.m. a mobile device ID therealchulo was used to access Green's account via IP address 172.56.10.104. At approximately 6:23 p.m., a mobile device user ID 5424325113269284 was used to access Jackson's account via IP address 99.203.69.2 and at approximately 7:32 p.m. a mobile device ID 5424325113269284 was used to access Jackson's account via IP address 97.70.38.142.

**Digital Video Snapshot**

Site: FTGA/46313 Alpharetta (GA)

Camera Group: 46313 Alpharetta

Camera Name: ATM

1/4/2019 6:23:53 PM (Eastern Standard Time)



Device Station ID: 2098

Case Note 1: DONOVAN GREEN DEP

\$5,567.73/PASIONIQUE JACKSON DEP \$5,843.13

(54) Based on the information I have obtained through this investigation, I believe that McElroy was utilizing a mobile device during each fraudulent transaction to store and retrieve usernames, passwords and debit card PINs in order to access the bank accounts. Each of the transactions in Georgia identified above occurred after seizure of the devices I seek authority to search, but based on the entire of the

investigation as discussed herein, including the large number of transactions and bank accounts involved, it is reasonable to conclude that McElroy, and his co-conspirators and accomplices, used mobile devices to assist in accessing bank accounts and conducting fraudulent transactions prior to seizure of the devices I seek authority to search and that those devices will contain evidence of criminal activity.

**EXECUTION OF SEARCH WARRANT  
AND FORENSIC EXAM**

(55) The electronic devices, further described in Attachment A, were seized by the West Bloomfield Police Department from XXX2 Silverbrooke West on February 9, 2018 and the Huron Township Police from Ezel McElroy and Mark Hobson on August 25, 2018, and are currently in the possession of United States Secret Service at the Detroit Field Office Cyber Lab located in Detroit, Michigan.

(56) As described above and in the attachments to this affidavit, this application seeks permission to search and seize

electronically stored information that the devices may contain, in whatever form the information is stored. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the internet are typically stored for some period of time on a device. Even when a user deletes information from a device, it can sometimes be recovered with forensics tools.

(57) I know from training and experience that searches and seizures of evidence from computers and mobile devices require agents to seize most or all items (hardware, software, passwords and instructions) to be processed later by a qualified computer expert in a laboratory or other controlled environment. Searching computer systems and mobile devices such as tablets and cellular telephones for criminal evidence requires experience in the computer field and a properly controlled environment in order to protect integrity of the evidence and recover even “hidden,” erased, compressed, password protected, or encrypted files. Because digital

evidence is extremely vulnerable to tampering or destruction (both from external sources and from destructive code imbedded in the system as a “booby trap”), the controlled environment of a laboratory is essential to its complete and accurate analysis. The USSS laboratory is located at the Cleveland Field Office located in Cleveland, Ohio.

(58) Searching for the evidence described in Attachment B may require a range of data analysis techniques. In some cases, agents and computer analysts may be able to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant. Criminals can mislabel or hide information, encode communications to avoid using key words, attempt to delete information to evade detection, or take other steps designed to frustrate law enforcement searches for information. These steps may require agents and law enforcement or other analysts with appropriate expertise

to conduct more extensive searches, such as scanning storage areas unrelated to things described in Attachment A, or perusing all stored information briefly to determine whether it falls within the scope of the warrant. In light of these difficulties, USSS intends to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in Attachment B.

(59) There is probable cause to believe that things that were once stored on the cellular telephone may still be stored there, for at least the following reasons:

(a) Based on my knowledge, training, and experience, I know that files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on an electronic device, the data contained

in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

(b) Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a device’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

(c) Wholly apart from user-generated files, storage media—in particular, electronic devices’ internal hard drives—contain electronic evidence of how a device has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Device users typically do not erase or delete this evidence,



because special software is typically required for that task.

However, it is technically possible to delete this information.

(d) Similarly, files that have been viewed via the internet are sometimes automatically downloaded into a temporary internet directory or “cache.”

(60) *Forensic evidence.* As further described, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the computer or cellular telephone, was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the computer or cellular telephones because:

(a) Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of

information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords.

Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the device was in use. Device file systems can record information about the dates files were created and the sequence in which they were created.

- (b) Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- (c) A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions

about how electronic devices were used, the purpose of their use, who used them, and when.

- (d) The process of identifying the exact electronically stored information on storage media that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators.

Whether data stored on a device is evidence may depend on other information stored on the device and the application of knowledge about how a device behaves.

Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- (e) Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

(61) *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the devices described in

Attachment A consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant. It would also authorize the seizure of electronic storage media, or potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).


(62) *Manner of execution.* Because this warrant seeks only permission to an examine device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

## CONCLUSION

(63) Based upon the information contained in this affidavit, your Affiant submits that there is probable cause to believe that images, records, evidence, fruits and instrumentalities

relating to the violation of the Specified Federal Offenses,  
may exist on the items held by the United States Secret  
Service (as more specifically described in Attachment A).

(64) WHEREFORE, your Affiant respectfully requests that a  
warrant be issued authorizing the agents of the United States  
Secret Service, with appropriate assistance from other law  
enforcement officers, to search the items identified in  
Attachment A and seize the items set forth in Attachment B,  
incorporated herein by reference.

  
Special Agent Matthew Lariviere  
United States Secret Service  
Affiant

Sworn to before me and signed in my  
Presence and/or by reliable electronic means.

Date: March 21, 2019



David R. Grand  
United States Magistrate Judge

**ATTACHMENT A**  
**DESCRIPTION OF PROPERTY TO BE SEARCHED**

1. The property to be searched is:
  - a. one (1) black Apple iPhone cellular device IMI #356769087236816 seized by the West Bloomfield Township Police Department on February 9, 2018;
  - b. one (1) rose-colored Apple Macbook laptop computer (serial number C02VG2HFHH27 ) seized by the West Bloomfield Township Police Department on February 9, 2018;
  - c. one (1) black iPhone cellular device IMI#354856093929633, seized by the Huron Township (Michigan) Police Department on August 25, 2018;
  - d. one (1) Samsung Galaxy cellular device IMI #359754071351554, seized by the Huron Township (Michigan) Police Department on August 25, 2018.
2. This warrant authorizes the forensic examination of these devices for the purpose of identifying and seizing the electronically stored information described in Attachment B and the copying and later review thereof pursuant to Federal Rule of Criminal Procedure 41(e)(2)(B). All electronics are being held by the United States Secret Service at the Detroit Field Office Cyber Lab located in Detroit, Michigan at the time of issuance of this warrant, but the search authorized herein may be conducted outside the Eastern District of Michigan pursuant to Federal Rule of Criminal Procedure 41(b)(2).

## **ATTACHMENT B**

### **DESCRIPTION OF ITEMS TO BE SEARCHED FOR AND SEIZED**

1. Cellular device hardware, software, documentation, passwords and data security, and electronically stored data, information, and records constituting evidence, fruits, or instrumentalities of violations of 18 U.S.C. §§ 371, (Conspiracy), 514 (fictitious obligations, security, make, utter, possess counterfeit security/check: make, utter, possess a forged security/check), 18 U.S.C. §§ 1343 (wire fraud), 1344 (bank fraud), and 1029 (access device fraud) (hereinafter “the Specified Federal Offenses”), including information related to the following:
  - a. identities, locations, and contact information for co-conspirators;
  - b. incriminating statements or messages made to and from the device’s owner or user;
  - c. text messages, including SMS/MMS messages and messages contained in messaging applications installed on the device or sent through internet-based services, such as Instagram, Facebook, Snapchat, Apple iMessage, WhatsApp, ICQ, and Kik, and emails to and from co-conspirators;
  - d. call log history, including numbers, dates, times, and duration;
  - e. electronic calendars;
  - f. digital voice recorded messages from co-conspirators;

- g. stored photos and video files relevant to the Specified Federal Offenses;
- h. internally stored GPS data;
- i. stored memos and scratch pad files pertaining to the Specified Federal Offenses;
- j. internet browser data, including favorites and history, pertaining to the Specified Federal Offenses;
- k. social media application data, including Facebook, Instagram, Snapchat, and Twitter, pertaining to the Specified Federal Offenses;
- l. the possession, manufacture, sale, or use of counterfeit/stolen/fraudulent checks, credit card accounts, or cellular service provider accounts;
- m. the purchase, sale, or use of items purchased with counterfeit/stolen/fraudulent checks, credit card accounts, or cellular service provider accounts;
- n. use or transfer of monetary instruments, including the laundering of monetary instruments, derived from items acquired from the use of counterfeit/stolen/fraudulent checks, credit card accounts; or cellular service provider accounts;
- o. lists of bank, financial institution, or cellular service provider customers and related identifying information;
- p. types, amounts, and prices of counterfeit/stolen/fraudulent checks or credit cards



produced, as well as dates, places, and amounts of specific transactions;

- q. sources of counterfeit/stolen/fraudulent check or credit card fraud information and materials (including names, addresses, phone numbers, account numbers, or any other identifying information);
  - r. any information recording schedules or travel; and
  - s. any bank records, checks, credit card bills, account information, and other financial records, including bitcoin.
2. Evidence of user attribution showing who used or owned the devices listed in Attachment A at the time things described in this warrant were created, edited, or deleted, such as user profiles logs, phonebooks, saved usernames and passwords, documents, and browsing history;
3. Records evidencing the use of the Internet Protocol addresses and device identifiers to communicate with bank websites and applications, including:
- a. Records of Internet Protocol addresses used;
  - b. Device identifier numbers assigned;
  - c. Records of internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form

of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

## UNITED STATES DISTRICT COURT

for the  
Eastern District of Michigan

Case: 2:19-mc-50420

Assigned To : Michelson, Laurie J.

Assign. Date : 3/21/2019

Description: RE: SEALED MATTER  
(EOB)

1

Case No.

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)2 Black I-phones; Mac Book; and Samsung Galaxy cell  
phone  
See Attachments for description.

## SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search  
of the following person or property located in the Eastern District of Michigan.  
(identify the person or describe the property to be searched and give its location):

See ATTACHMENT A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property  
described above, and that such search will reveal (identify the person or describe the property to be seized):

See ATTACHMENT B.

**YOU ARE COMMANDED** to execute this warrant on or before April 4, 2019 (not to exceed 14 days)☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the  
person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the  
property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory  
as required by law and promptly return this warrant and inventory to the presiding United States Magistrate Judge on duty.  
(United States Magistrate Judge)☒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.  
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose  
property, will be searched or seized (check the appropriate box)☒ for 30 days (not to exceed 30) ☐ until, the facts justifying, the later specific date of \_\_\_\_\_.Date and time issued: March 21, 2019 5:10 pm

Judge's signature

City and state: Detroit, MichiganDavid R. Grand U. S. Magistrate Judge

Printed name and title

**Return**

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

**Certification**

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: \_\_\_\_\_

\_\_\_\_\_  
*Executing officer's signature*\_\_\_\_\_  
*Printed name and title*